

BlackHole: Manual de Instalación y Configuración.

Nicolas Rebagliati

Guía para instalación y configuración de BlackHole.

Indice

Resumen:

Blackhole fue ideado para solucionar un problema que teníamos donde trabajo.
Nuestro problema era que teníamos una plataforma muy grande de servidores, y una gran cantidad de usuario que necesitaban conectarse a ellos. Mayormente para dar soporte.
Además esta gente solía variar bastante seguido, por lo cual teníamos dos opciones.
Crear usuarios a todos en todos los servidores (eran demasiados) o creábamos un usuario genérico para todos.
La primera opción era inviable, sobre todo por la alta rotación de usuarios.
Y la segunda era claramente insegura, porque no había forma de tracear que hacia cada usuario ni a donde estaba conectado.

Necesitábamos algo que fuera fácil de administrar y nos diera la visibilidad de poder tener control de que hacían los usuarios.

Como funciona?
Blackhole principalmente es un frontend, todos los usuarios deben conectarse mediante este servidor.
Y la aplicación esta configurada como shell de los usuarios, para que sea lo único que pueden ejecutar.
En la base de datos se encuentra la información de todos los servidores que tenemos, agrupados por ambientes.
También están las llaves privadas que va a usar para cada conexión dependiendo del usuario.
Luego cada usuario tiene un perfil asociado a los servidores con los que cada usuario tiene permiso para conectarse.

La aplicación es un menu en curses, con la lista de los servidores habilitados.
Los cuales podemos recorrer y conectarnos al que queramos.

Pero es mucho mas que eso, porque blackhole guarda información de cada conexión que se establece.

- Que usuario
- Como que usuario se conecto
- Hora del login
- Hora del logout
- Duración de la conexión
- El uso (la cantidad de comandos que ejecuto/el tiempo de conexión)
- La cantidad de teclas que oprimió

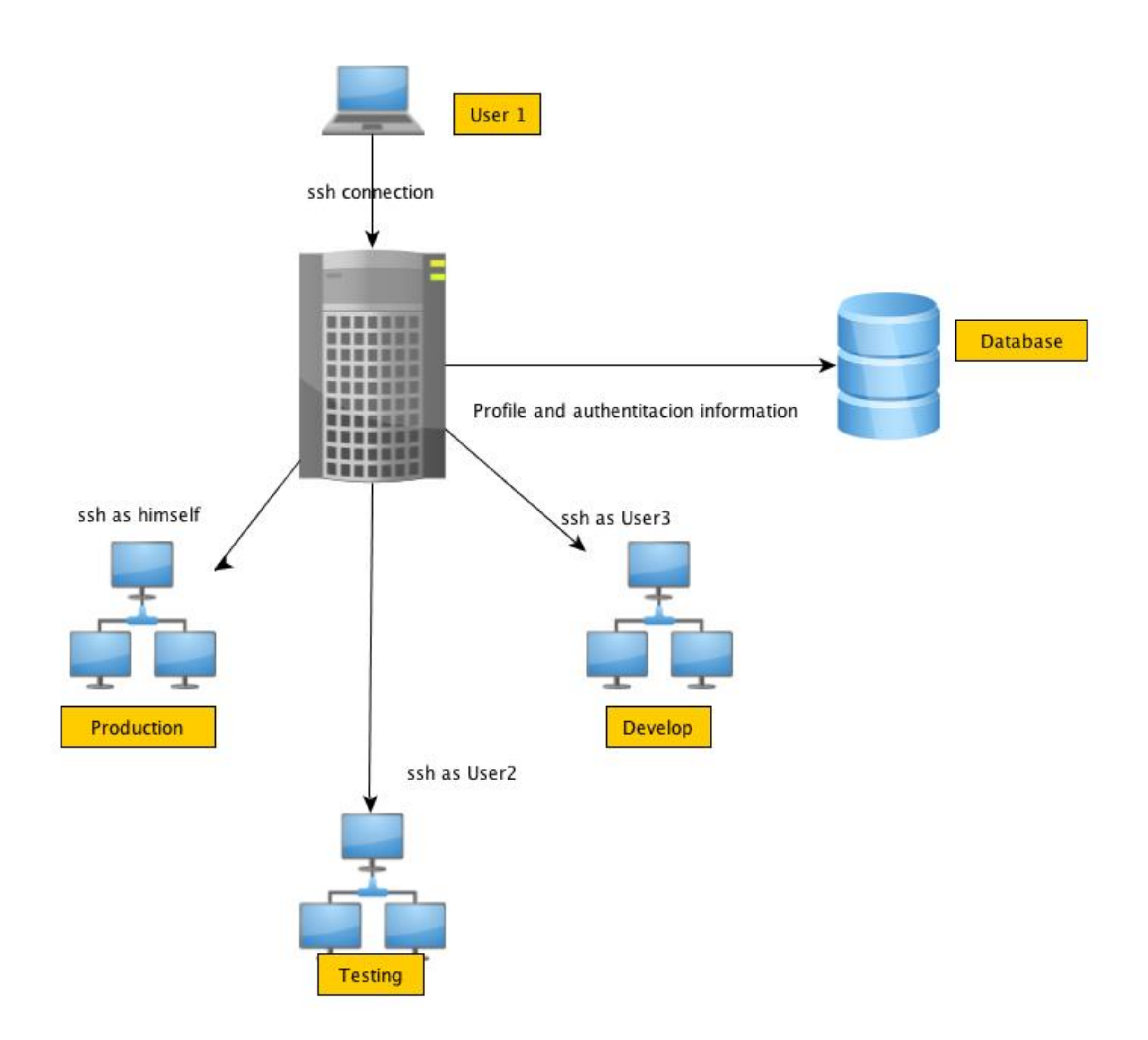
Pero además guarda un log de todo el contenido de cada conexión.

Toda esta información puede ser vista desde la web que trae integrada, donde genera gráficos y a su vez nos permite descarga el log de cada conexión.

Funcionalidad Extras:

Aparte de lo mencionado, Blackhole tiene otras funcionalidades.

- Servidor de Chat, donde los usuarios conectados pueden hablar.
- Validación por token, opcionalmente se puede activar la validación por token (que es enviado por mail), y hasta que no es ingresado correctamente el usuario no puede acceder.
- Habilitación de usuario por rango horario, o a un grupo restringido de servidores.



Instalación:

El proceso de instalación es un poco complejo, ya que posee varias dependencias.
La aplicación esta escrita en python y esta basada en el framework Django.
Corre sobre Linux (testeado), OSX (testeado) o cualquier otro unix que cumpla con las dependencias.
En este manual se muestra una instalación desde cero.
La instalación se hizo sobre un Linux (Ubuntu 12.04) con LAMP (Mysql-Apache-PHP), Django 1.4 (se desarrollo y se probo con esta versión, aunque puede ser que funcione con inferiores. Pero no lo se), python 2.7 (con 2.6 debería funcionar sin problemas).

Primero de todo es instalar todas las dependencias.

- Django (https://www.djangoproject.com/)
- Paramiko
- MysqlDB
- Urwid
- python-simplejson
- django-qsstats-magic
- python-dateutil
- django_extensions
- libapache2-mod-wsgi (Solo si queremos usar apache)

La mayoría podemos instalarlos mediante apt.
Yo recomiendo Django instalarlo mediante el tarball del su sitio web.

apt-get install python-mysqldb python-paramiko python-urwid python-simplejson libapache2-mod-wsgi

Hay 3 que debemos utilizar pip (Python Package Index):
pip install django-qsstats-magic python-dateutil django_extensions smpplib

Con esto listo, tenemos que crear la base de datos y un usuario. (Para esto no hay instrucciones, recomiendo instalar phpmyadmin y hacer desde ahí).
En este manual se utilizara una base llamada blackhole, con un usuario y password blackhole/blackhole.
Recomiendo poner un password mas seguro en producción.

El próximo paso es instalar la aplicación.
Como la aplicación se ejecutara como Shell de los usuarios, la vamos a instalar en el /home. Pero puede ser donde quieran

cd /home
tar zxvf BlackHole.tgz

Debemos crear un grupo (ejemplo blackhole), el cual debe ser grupo primario de todos los usuario que usen la aplicación.
groupadd blackhole

Ahora es muy importante modificar los permisos.

cd /home/blackHole
chown –R root:blackhole ./

Fin de la instalación.

Configuración:

Configuración de directorios:

El próximo paso es la configuración, lo primero que debemos hacer es modificar el archivo de configuración llamado blackhole.config, ubicado en /home/BlackHole/

Este es su contenido

[settings]
debug = False
application_path = /home/BlackHole
log_path = /home/BlackHole/logs
chat_enabled = True
token_validation_enabled = False

Debemos modificar la entrada **application_path** para que sea igual a donde instalamos la aplicación.
Y la entrada **log_path** es el directorio donde queremos que se guarden los logs de las sesiones.
Es muy importante asegurarse que ese directorio tenga permisos de escritura para el grupo blackhole.

NOTA: los logs se van a guardar en este directorio, pero van a intentar primero ser escritos en un directorio con el nombre del Perfil del usuario dentro de este directorio. En caso de no existir dicho directorio, se guardaran en el directorio indicado por log_path.
Esos directorio deben ser creados a mano, y también deben tener permisos de escritura para el grupo blackhole.

Aquí también se configura si queremos habilitar la opción de chat, y la opción de token.
La habilitación de token que se encuentra qui es a nivel global, ya que luego se puede habilitar la opción a cada usuario.

Configuración de la Base de Datos:

Una vez que tenemos creada la base de datos y el usuario.
Tenemos que ingresarlo en el archivo: /home/BlackHole/black_hole/settings.py
Donde dice "DATABASES", debemos ingresar:

- "NAME": el nombre de la base de datos creada
- "USER": el nombre del usuario creado
- "PASSOWRD": el password del usuario creado

NOTA: Adicionalmente en este archivo podemos cambiar el TimeZone.
Ejemplo: TIME_ZONE = 'America/Chicago'
Y el idioma. Ejemplo: LANGUAGE_CODE = 'en-us'
Actualmente los únicos idiomas habilitados son Ingles (en-us) y español de Argentina (es-AR).

Una vez que eso esta listo, tenemos que crear las tablas.
Para esto tenemos que ejecutar el siguiente comando:
cd /home/BlackHole
./manage.py syncdb

y luego para cargar algunas configuraciones necesarias:
./manage.py initial_setup

Configuración del web server:

Para correr el sitio web integrado con blackhole tenemos 2 opciones.
Correrlo con apache, o correrlo mediante el webserver incorporado con django (La cual no es recomendable).

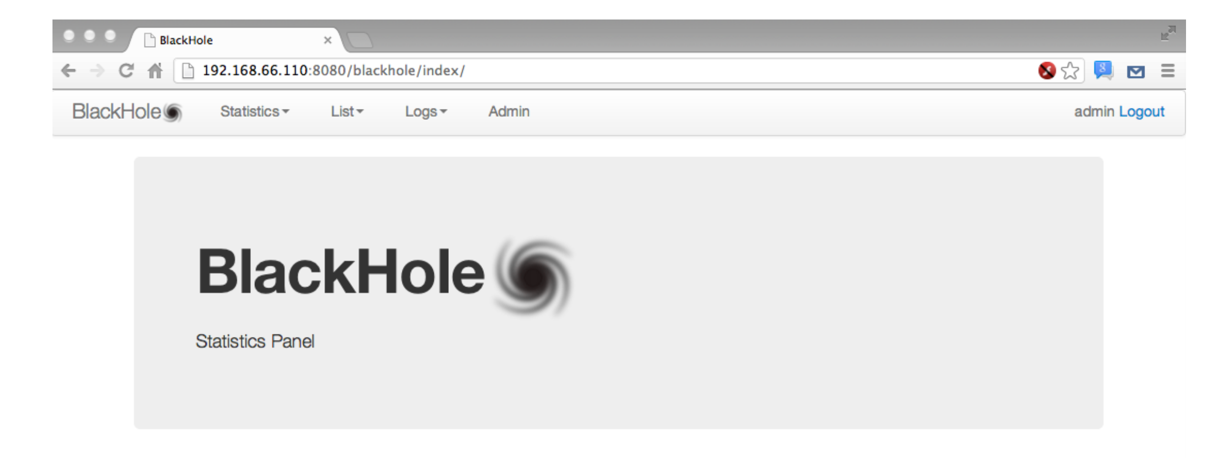
Para hacer mas fácil la integración con apache, se entregan 2 archivos de configuración necesarios.
Los mismo se encuentran en "/home/BlackHole/apache"
En django.wsgi solo debemos modificar el directorio de instalación si no es el mismo usado en este manual.

El archivo site.example debe ser copiado al directorio de sites-available de apache, y luego ser habilitado (si se modifico el directorio de instalación, también se debe modificar en este archivo):
cp site.example /etc/apache2/sites-available/blackhole
a2ensite blackhole

En el archivo de configuración de ejemplo se utiliza el puerto 8080, por lo cual debemos habilitar dicho puerto en apache agregando esto en el archivo /etc/apache2/ports.conf
NameVirtualHost *:8080
Listen 8080

Ya podemos reiniciar el apache y la web esta funcionando.

Podemos ingresar a ella mediante esta url:
http://localhost:8000/blackhole/index/
Con el usuario y password que creamos anteriormente al crear la base de datos.



Configuración de la aplicación:

Ahora se debe cargar toda la información referente a los usuario, servidores, llaves etc.

Al hacer click en el botón "Admin", nos llevara a esta pagina:



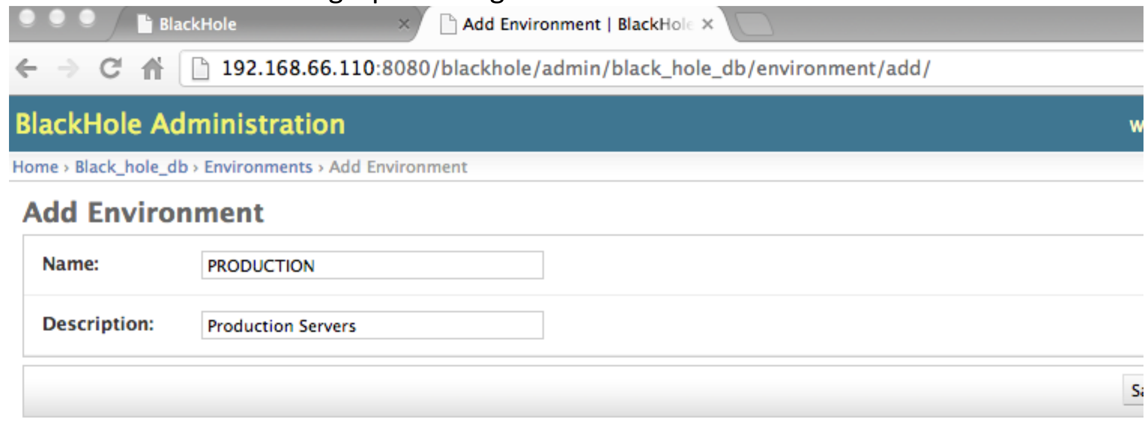
Hay que hacer una diferenciación entre "Auth->Users" y "Black_Hole_Db->Users".
En la primer opción se deben crear los usuario que van a administrar la aplicación únicamente.
Los segundos son los usuarios que la van a utilizar.
Asi mismo se pueden crear grupos para usuarios de administración que puedan hacer tareas puntuales.
Como por ejemplo habilitar y deshabilitar usuarios, pero únicamente eso.

Usuarios Administradores:

En Auth->Users, debemos crear esos usuarios administrativos. Recordar que para que esos usuario puedan entrar a esta web debe estar activada la opción "Staff".
Si no queremos utilizar grupo, y los usuarios deben tener acceso a modificar todo. En lugar de darles permisos puntuales, se los puede habilitar como "Superuser".

Ambientes (Environment):

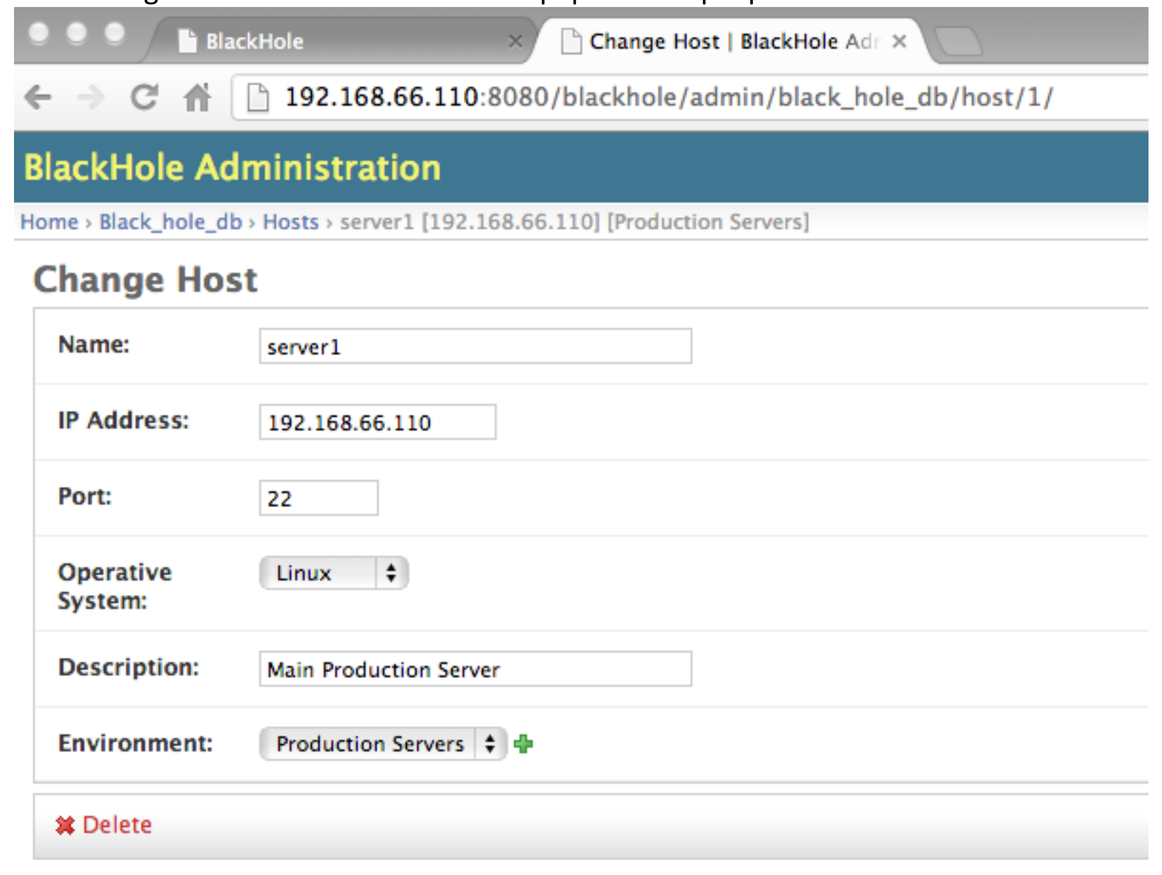
Los ambientes son una agrupación lógica de los servidores.



NOTA: No utilizar espacios en el campo NAME, ya que el mismo se utilizara para los directorios de los logs y puede traer problemas.

Equipos (Host):

Es la configuración de cada uno de los equipos a los que podremos conectarnos.

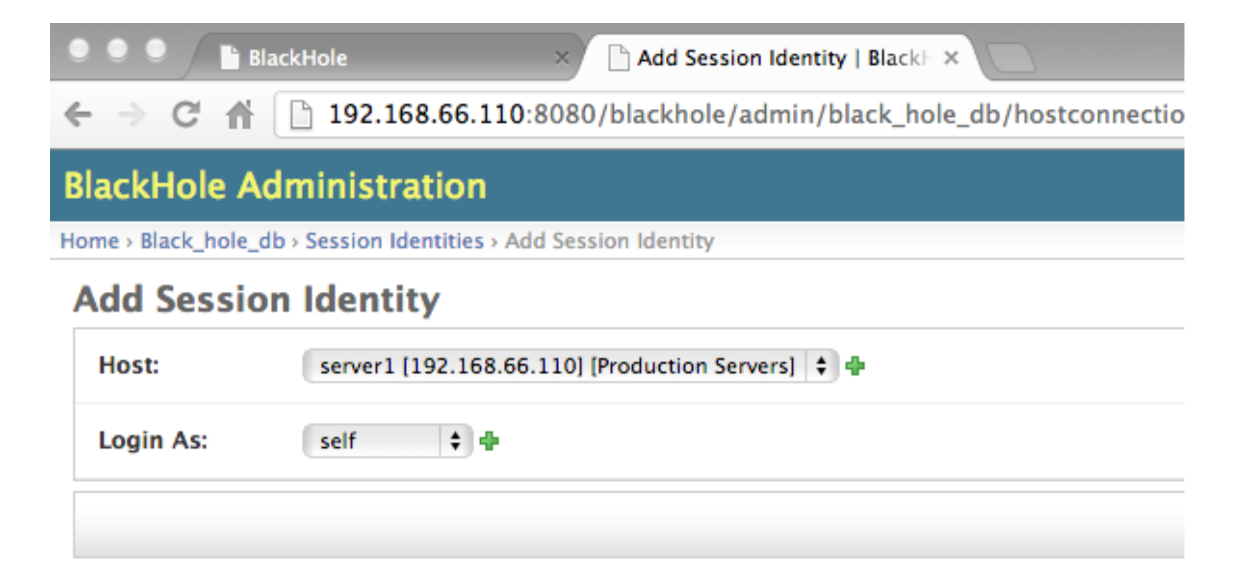


Identidad de Usuario (User Identity):

La identidad de usuario es un concepto fundamental que debe ser comprendido muy bien.
La identidad de usuario es el usuario que va a usar para conectarse al equipo seleccionado.
Por default viene creada una identidad llamada "self".
Las identidades que deben ser creadas son los usuarios genéricos.
Por ejemplo si tenemos usuarios que se conectan con sus propios usuarios personales, entonces ellos van a usar la identidad "self".
Ejemplo, si tenemos un usuario llamado John y en el servidor A se tiene que conectar con el usuario John, para ese equipo va a tener que conectarse como "self".
Pero si ese mismo usuario en el servidor B se conecta como el usuario admin, para ese servidor va a tener que conectarse con la identidad "admin". Y esa debe estar creada aquí, pero no la identidad John.

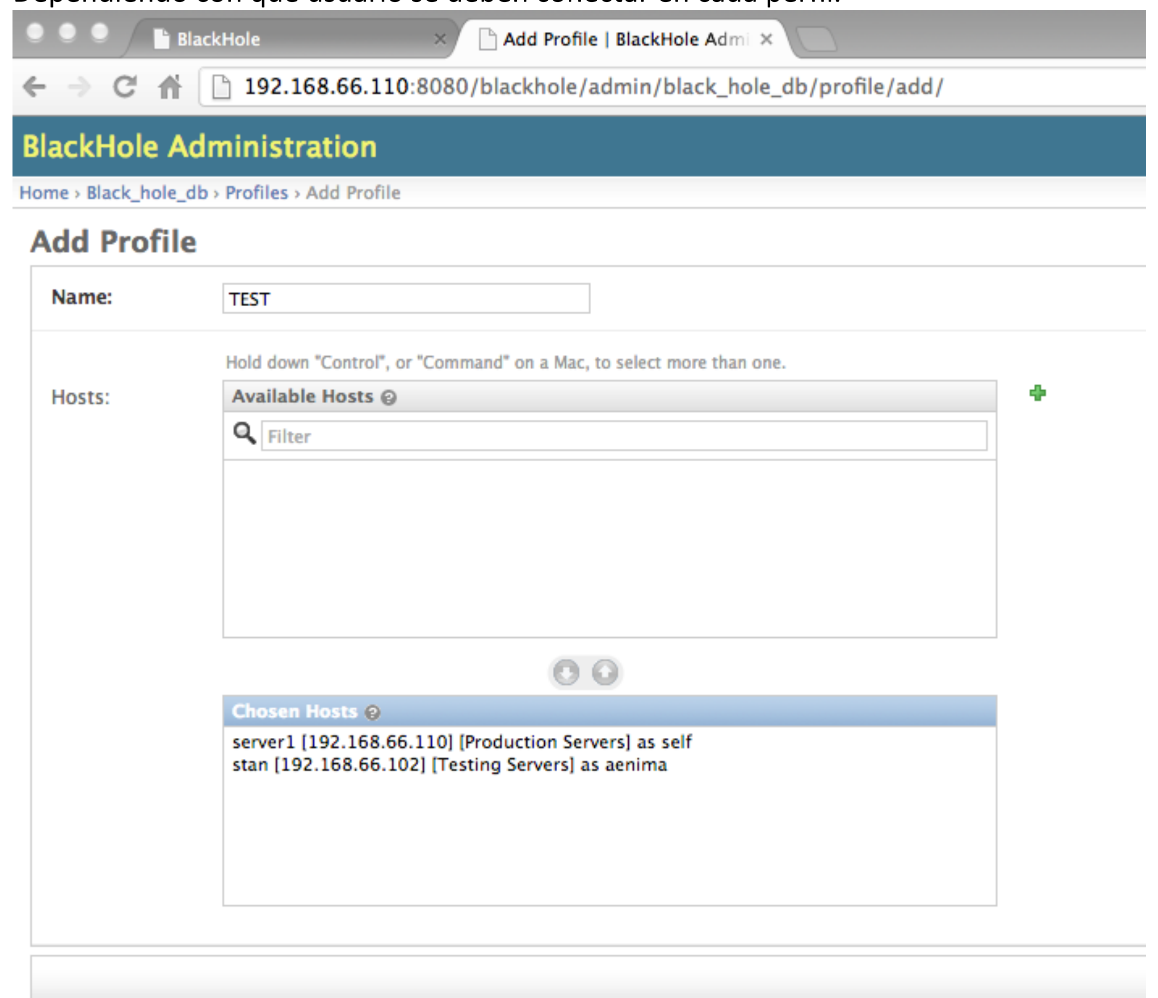
Identidad de Sesión (Session Identity):

La identidad de sesión es otro concepto importante, es lo que va a asociar una Identidad de Usuario a un equipo.
Luego los Perfiles lo que van a tener son una o mas "Identidades de Sesión" asociadas.



Perfil (Profile):

Aquí creamos los distintos perfiles de usuarios.
En ellos seleccionamos que Identidades de Sesión deben estar asociados a cada uno.
Dependiendo con que usuario se deben conectar en cada perfil.

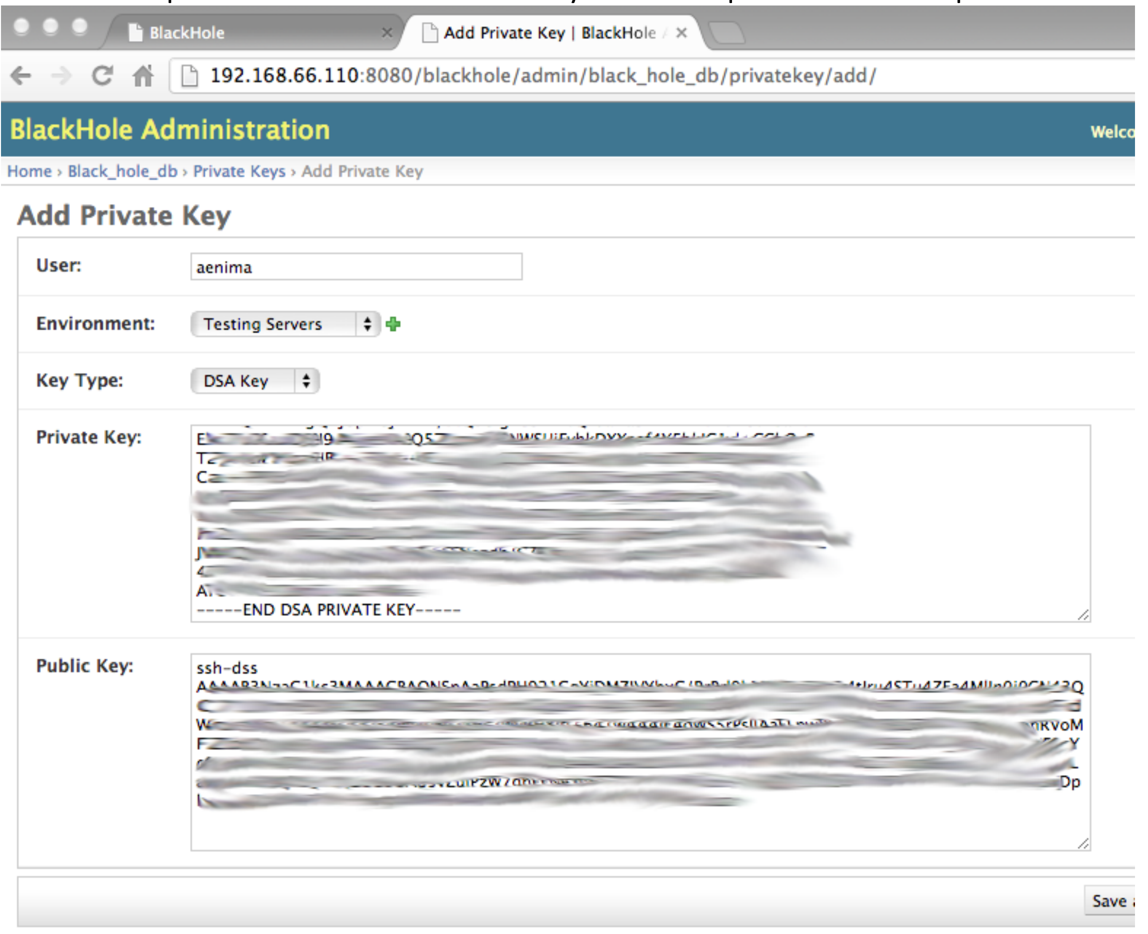


Llave Privada (Private Key):

Las llaves privadas son el medio que utilizara para conectarse a los servidores.
La llaves privadas son por ambiente, por lo cual en nuestros servidores de un mismo ambiente debemos tener cargadas las mismas llaves publicas para un usuario que deba conectarse a uno o mas servidores de ese ambiente.
Una cosa importante es que las lleves deberán estar creadas de esta manera.
Ejemplo si yo tengo 2 identidades de sesión:

- John -> server1(PRODUCCION) ->como self
- John -> server2(PRODUCCION) -> como admin

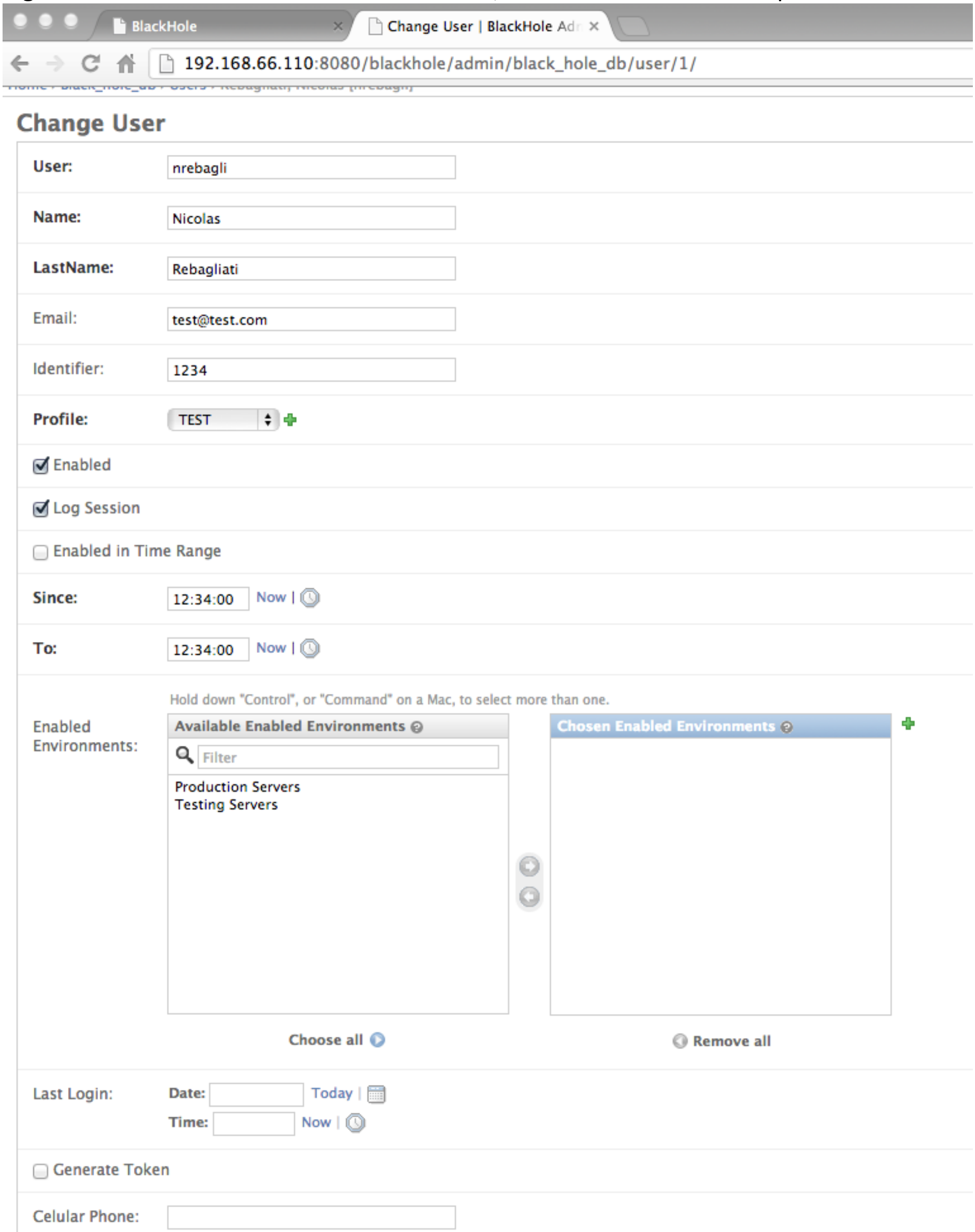
Entonces debo tener 2 llaves creadas
La de admin para el ambiente PRODUCCIO y la de John para el ambiente producción.



Es muy importante seleccionar el tipo correcto de llave (DSA o RSA).

Usuario (User):

El usuario tiene varios campos que son opcionales, y solo son útiles si se utilizan algunas funcionalidades extras de BlackHole, como lo es la validación por token.

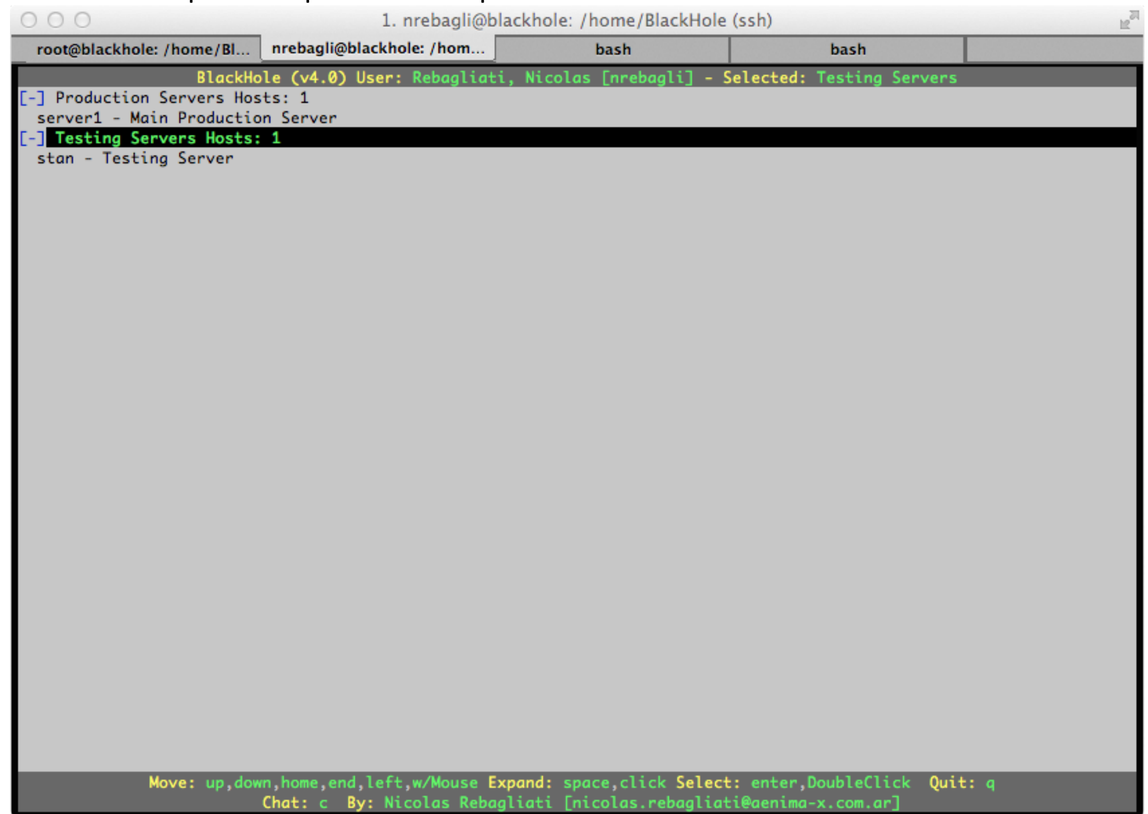


El campo email no es obligatorio, pero si se desea utilizar token por email debe estar completo.
El campo identifier es alguna clase de identificador del usuario. Pero tampoco es obligatorio.
Cuando un usuario esta deshabilitado, no podrá conectarse a ningún servidor.

Pero existe otra opción, que es la de habilitarlo en un rango horario, y si esta fuera de ese rango no podrá ingresar a ningún servidor.
Para que esta opción funcione, el usuario tiene que estar habilitado.
Ya que esa opción es evaluada antes que esta.
También se puede restringir a los ambientes que puede logearse, de esta manera por mas que el usuario tenga permisos para entrar a otros servidores, no va a poder.
El campo de Celular es para poder enviar token por SMS. No es obligatorio.
Y por ultimo la opción Log Session, es para poder deshabilitar a algún usuario puntual que no se guarde su sesiones en archivos (aunque igualmente se guardaran en la base de datos para estadísticas).

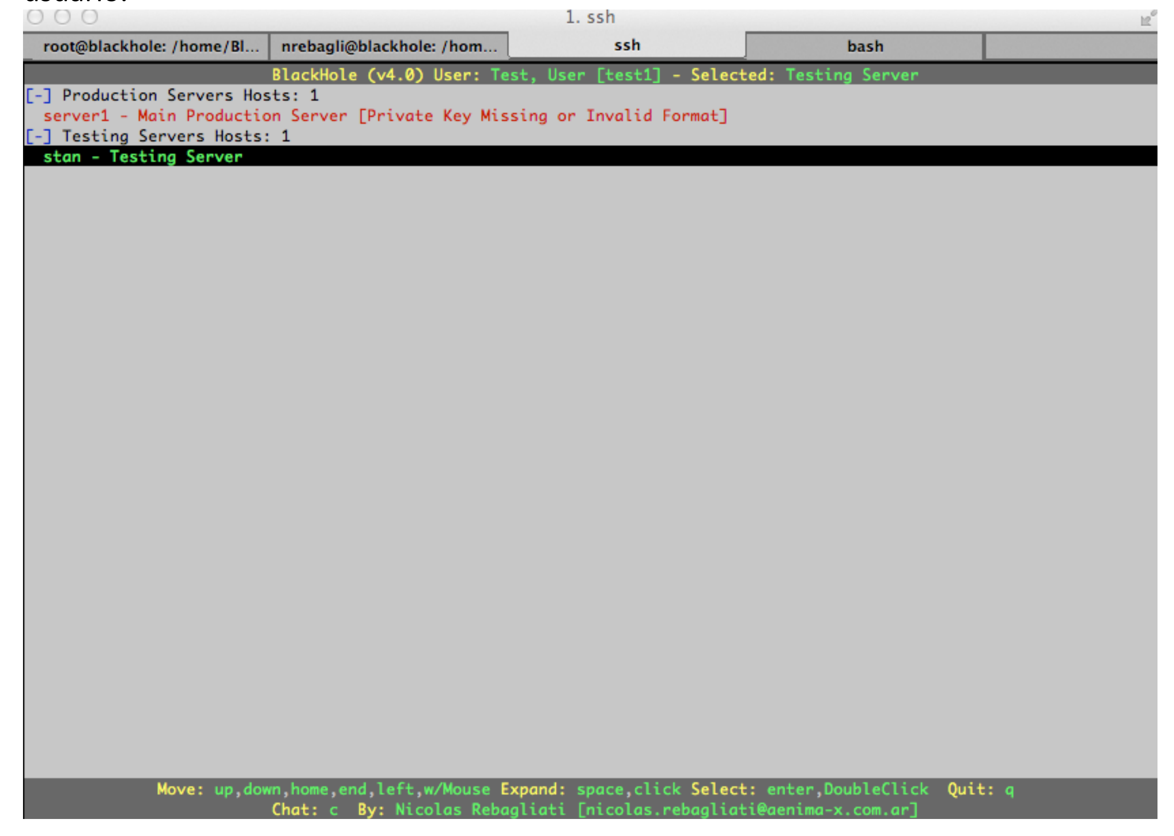
Uso:

Cuando todo este listo, los usuarios se van a conectar por ssh a blackhole y este les brindara las opciones que tienen disponibles.



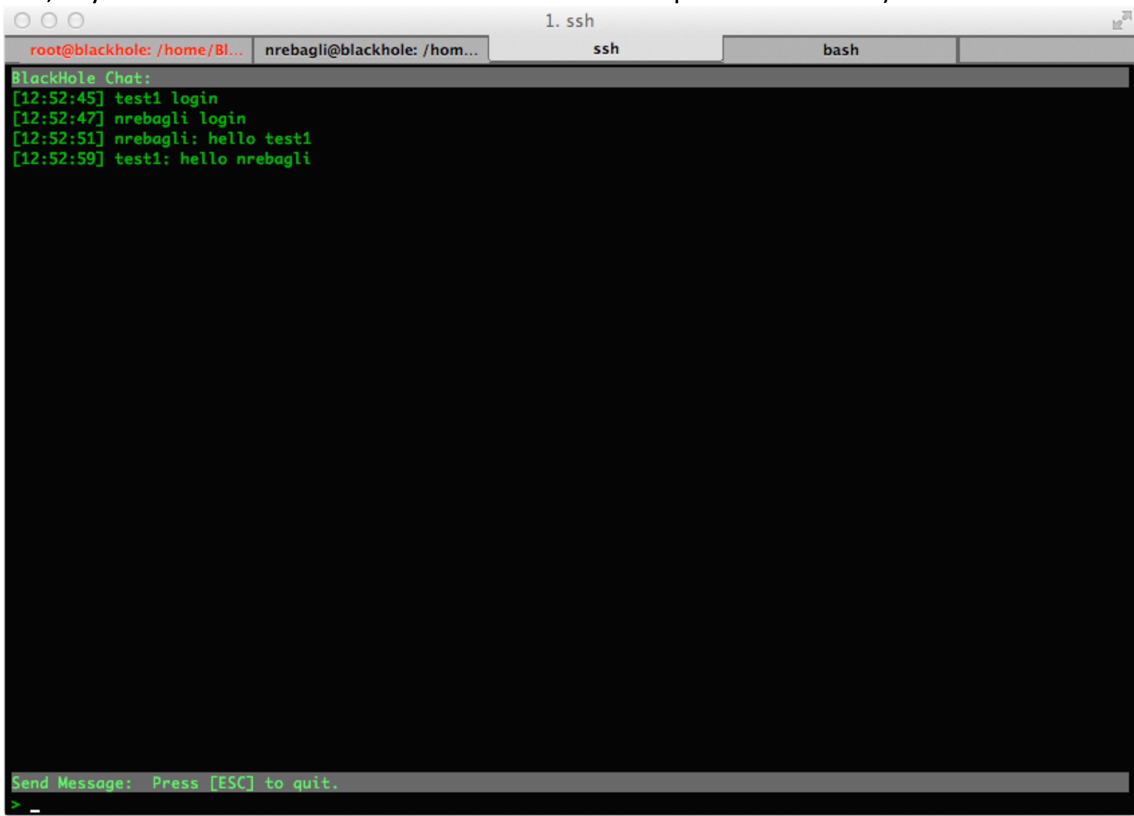
Es desplazamiento se puede hacer con el teclado o con el mouse.
Cuando un usario termine su conexión ssh, con el servidor que selecciono, va a ser llevado nuevamente a este menú.

Si al querer conectarse llega a haber un problema con alguna llave se le va a indicar al usuario.



Chat:

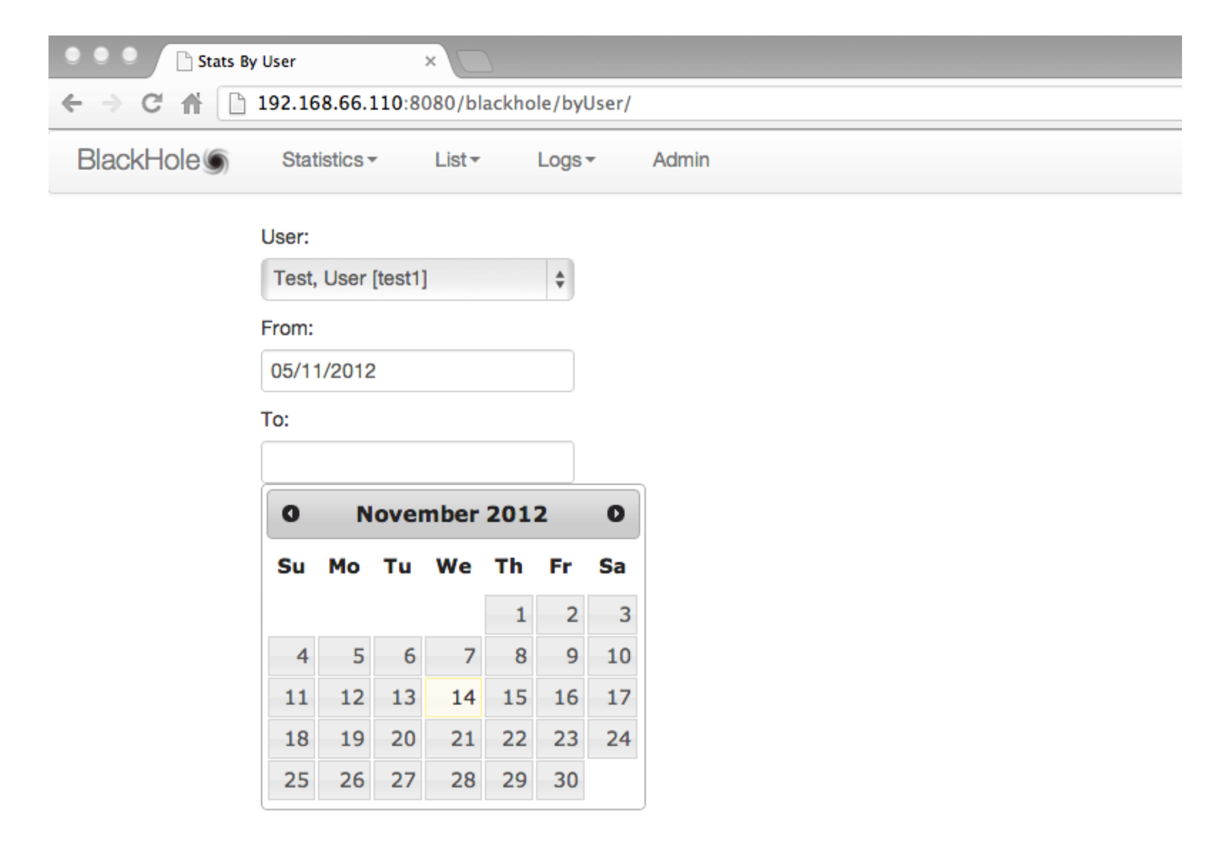
Si se habilita la opción del chat incorporado los usuarios podrán desde el menú principal entrar a un chat para hablar entre ellos (los usuario podrán conectarse una vez, si ya tiene en otra conexión un chat abierto no podrá abrir otro).



Para poder conectarse al chat debe estar corriendo el proceso del chatServer:
cd /home/BlackHole
nohup ./startChatServer.py &

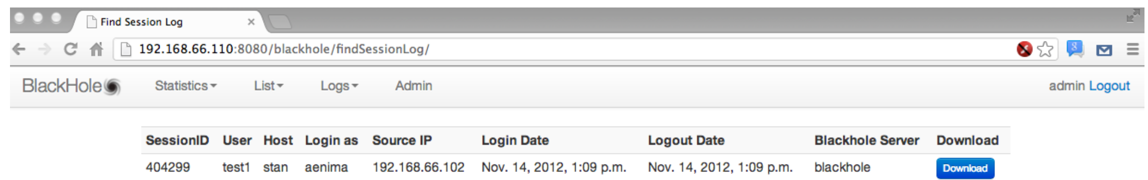
Web:

En estadisticas encontraremos muchas estadísticas, que pueden ser sacadas por usuario o por servidor.



De todas podemos seleccionar un rango horario y el tipo de estadística a buscar para que nos genere un grafico.

En la opción de logs podemos encontrar la opción para buscar las sesions de un usuario determinado en un rango horario y luego poder descargar el log de cada sesión.



Algunos ejemplos:

Statistics ×

192.168.66.110:8080/blackhole/byUser/

BlackHole Statistics List Logs Admin

User: Test, User [test1]

From: Nov. 13, 2012

To: Nov. 16, 2012

Clear selection

Zoom to selection.

Back

Logins

2.5 2.0 1.5 1.0 0.5 0.0

Nov 13 8:00 | Nov 13 16:00 | Nov 14 0:00 | Nov 14 8:00 | Nov 14 16:00 | Nov 15 0:00 | Nov 15 8:00 | Nov 15 16:00 | Nov 16 0:00

Statistics ×

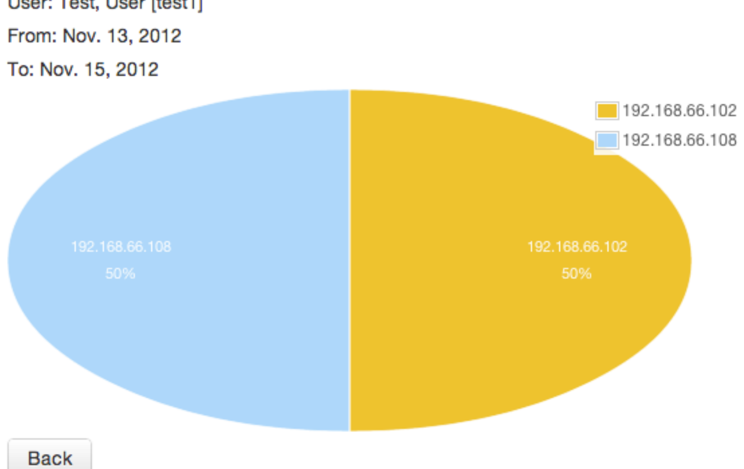
192.168.66.110:8080/blackhole/byUser/

BlackHole Statistics List Logs Admin

User: Test, User [test1]

From: Nov. 13, 2012

To: Nov. 15, 2012



Back

Extras:

Como comente antes existen algunas funcionalidades extras que no están habilitadas.

- Validación de la web por radius (ver las notas en settings.py)
- Envió de token por mail, además de habilitarlo en el archivo de configuración se debe modificar las credenciales en /home/BlackHole/black_hole_gui/emailSender.py
- También se pueden enviar token por sms, pero para esto se debe tener acceso a SMSC. Si se requiere se debe modificar la configuración en /home/BlackHole/black_hole_gui/smsSender.py

Ante cualquier duda de estas opción no duden en mandarme un correo.

Bugs conocidos:

Aun quedan varias cosas para solucionar, los principales son:

- No se pueden poner en un perfil 2 Identidades de sesión de un mismo equipo. Sino blackhole va a tener un problema al generar el menú y este va a comportar de manera extraña. Si necesitamos que un usuario se pueda conectar al mismo servidor con 2 usuario diferente lo que debemos hacer es crear ese equipo 2 veces con diferentes nombres y crear 2 identidades de sesión.
- El tamaño de la terminal al conectarnos desde BlackHole a otro servidor será del mismo tamaño que la ventana de BlackHole. Si modificamos el tamaño antes de conectarnos a algún servidor se ajustara también, pero si modificamos el tamaño de la ventana luego se habernos conectado al otro servidor esa terminal continuara teniendo su tamaño original.
- Si el servidor donde corre Blackhole no es muy potente, puede ser que cuando tengamos muchos usuarios conectados y alguno ejecute algún comando que escriba mucho por pantalla (Ejemplo “ejecutar un select * from table”), puede ser que los demás usuarios sientan que esta lento. Es porque eta consumiendo muchos recursos para escribir en pantalla y en el log de la sesión. Por eso se recomienda no correrlo en maquina virtuales su se espera tener muchos usuarios.